

1 This listing of claims will replace all prior versions, and listings, of claims
2 in the application:

3
4 Listing of Claims

5
6 Claims 1-175 (Canceled)

7
8 Claim 176 (Previously presented): In a networked client-server
9 environment, apparatus for use in conjunction with a digital rights management
10 system, the apparatus comprising:

11 a client computer connected to the network, the client computer having:

12 a processor;

13 a memory having computer executable instructions stored therein;

14 and

15 an enforcer, contained within the digital rights management system,
16 for controlling use of watermarked software objects, wherein the enforcer
17 stores a predefined watermark key which defines a specific one of a
18 plurality of identical watermarks embedded in the watermarked software
19 object with different watermark keys to be used by the enforcer in
20 subsequently controlling use of each one of said watermarked software
21 objects, and wherein the predefined watermark key expires after a
22 predefined period of time elapses since said predefined watermark key was
23 initially stored in the enforcer;

24 wherein the processor, in response to the stored executable
25 instructions:

establishes a network connection to a watermark key;

issues a request to the server for a new watermark key; and

utilizes either the predefined watermark key or the new

1 watermark key, as received from the server, for the predefined
2 watermark key for subsequent use in controlling access to the
3 watermarked software objects until such time as the predefined key
4 has expired after which the new watermark key is used instead; and
5 the server, connected to the network, which, in response to the
6 request:

7 selects, if the predefined watermark key has not been revoked
8 for the client computer, another one of predefined plurality of
9 predetermined watermark keys for use in controlling access to the
10 software watermarks objects as the new watermark key;

11 sends the new watermark key to the client computer; and

12 if the predefined watermark key has been revoked, does not
13 supply the new watermark key to the client computer.

14 Claim 177 (Original): The apparatus in claim 176 wherein the network
15 connection comprises a secure connection.

16 Claim 178 (Original): The apparatus in claim 177 wherein the server is
17 associated with a publisher of any one of the watermarked software objects or a
18 vendor of said one object, or a watermarking authority.

19 Claim 179 (Original): The apparatus in claim 178 wherein:

20 the client computer, in response to the stored instructions and in conjunction
21 with the request, also supplies the server with an existing certificate for predefined
22 public key associated with the client computer; and

23 the server, if the existing certificate for the public key has not been revoked
24 by the server, provides the client computer with the new watermark key.

1 Claim 180 (Previously presented): In a networked client-server
2 environment, a method for use in conjunction with a digital rights management
3 system,

4 in a client computer connected to a network, the client computer having: a
5 processor; a memory having computer executable instructions stored therein; and
6 an enforcer, contained within the digital rights management system, for controlling
7 use of watermarked software objects, wherein the enforcer stores a predefined
8 watermark key which defines a specific one of a plurality of identical watermarks
9 embedded in the watermarked software object with different watermark keys to be
10 used by the enforcer in subsequently controlling use of each one of said
11 watermarked software objects, and wherein the watermark key expires after a
12 predefined period of time elapses since said key was initially stored in the
13 enforcer; wherein the method comprises the steps, upon expiration of the
14 watermark key, performed by the processor, in response to the stored executable
15 instructions, of:

16 establishing a network connection to a server;

17 issuing a request to the server for a new watermark key; and

18 utilizes either the predefined watermark key or the new watermark
19 key, as received from the server, for the predefined watermark key for
20 subsequent use in controlling access to the watermarked software objects
21 until such time as the predefined watermark key has expired after which the
22 new watermark key is used instead; and

23 in the server, connected to the network and, in response to the request, the
24 steps of:

25 selecting, only if the predefined watermark key has not been revoked
for the client computer, another one of a predefined plurality of
predetermined watermark keys for use in controlling access to the software
watermarks objects as the new watermark key;

1 sending the new watermark key to the client computer; and
2 if the predefined watermark key has been revoked, not sending the
3 new watermark key to the client computer.

4 Claim 181 (Original): The method in claim 180 wherein the network
5 connection comprises a secure connection.

6
7 Claim 182 (Original): The method in claim 181 wherein the server is
8 associated with a publisher of any one of the watermarked software objects or a
9 vendor of said one object, or a watermarking authority.

10 Claim 183 (Original): The method in claim 182 further comprising the
11 steps of:

12 in the client computer and in response to the stored instructions and in
13 conjunction with the request:

14 supplying the server with an existing certificate for a predefined
15 public the client computer; and

16 in the server, if the existing key associated with certificate for the public
17 key has not been revoked by the server, providing the client computer with a new
18 certificate, for the new watermark key.

19 Claim 184 (Previously presented): In a networked client-server
20 environment, apparatus for obtaining a watermark key for use in a digital rights
21 management system, the apparatus comprising:

22 a client computer connected to the network, the client computer having:

23 a processor;

24 a memory having computer executable instructions stored therein;

25 and

1 an enforcer, contained within the digital rights management system,
2 for controlling use of watermarked software objects, wherein the enforcer is
3 capable of storing a predefined watermark key which defines a specific one
4 of a plurality of identical watermarks embedded in the watermarked
5 software object with different watermark keys to be used by the enforcer in
6 subsequently controlling use of each one of said watermarked software
7 objects;

8 wherein, if the enforcer does not then possess the watermark key, the
9 processor, in response to the stored executable instructions:

10 establishes a network connection to a server;

11 issues a request to the server for a watermark key; and

12 stores the watermark key, received from the server, within the
13 enforcer for subsequent use in controlling access to watermarked software
14 objects; and

15 the server, connected to the network, which, in response to the request:

16 selects, one of the a predefined plurality of predetermined watermark
17 keys for use in controlling access to the software watermarked objects as
18 the watermark key;

19 downloads the watermark key to the client computer.

20 Claim 185 (Original): The apparatus in claim 184 wherein the request
21 contains a public key associated with the client computer and

22 the server, in response to the request:

23 encrypts the watermark key using the public key of the client
24 computer so as to yield the encrypted key; and

25 downloads the encrypted key to the client computer as the watermark
key; and

the client computer:

1 upon receipt of the watermark key, decrypts the encrypted key using
2 a private key associated with the client computer so as to yield a decrypted
3 key;

4 and stores the decrypted key as the watermark key.

5 Claim 186 (Original): The apparatus in claim 185 wherein the network
6 connection comprises a secure connection.

7
8 Claim 187 (Original): The apparatus in claim 186 wherein the server is
9 associated with a publisher of any one of the watermarked software objects or a
10 vendor of said one object, or a watermarking authority.

11 Claim 188 (Previously presented): In a networked client-server
12 environment, a method for obtaining a watermark key for use in a digital rights
13 management system,

14 in a client computer connected to a network, the client computer having: a
15 processor; a memory having computer executable instructions stored therein; and
16 an enforcer, contained within the digital rights management system, for controlling
17 use of watermarked software objects, wherein the enforcer is capable of storing a
18 predefined watermark key which defines a specific one of a plurality of identical
19 watermarks embedded in the watermarked software object with different
20 watermark keys to be used by the enforcer in subsequently controlling use of each
21 one of said watermarked software objects; wherein the method comprises the
22 steps, performed by the processor if the enforcer does not then possess the
watermark key and in response to the stored executable instructions, of:

23 establishing a network connection to a server;

24 issuing a request to the server for a watermark key; and

25 storing the watermark key, received from the server, within the

1 enforcer for subsequent use in controlling access to watermarked software
2 objects; and in the server, connected to the network and in response to the
3 request:

4 selecting, one of a predefined plurality of predetermined watermark
5 keys for use in controlling access to the software watermarked objects as
6 the watermark key;

7 downloading the watermark key to the client computer.

8 Claim 189 (Original): The method in claim 188, wherein the request
9 contains a public key associated with the client computer, comprising the steps of:

10 in the server, in response to the request:

11 encrypting the watermark key using the public key of the
12 client computer so as to yield the encrypted key; and

13 downloading the encrypted key to the client computer as the
14 watermark key; and

15 in the processor, in response to the stored instructions:

16 upon receipt of the watermark key, decrypting the encrypted
17 key using a private key associated with the client computer so as to
18 yield a decrypted key; and

19 storing the decrypted key as the watermark key.

20 Claim 190 (Original): The method in claim 189 wherein the network
21 connection comprises a secure connection.

22 Claim 191 (Original): The method in claim 190 wherein the server is
23 associated with a publisher of any one of the watermarked or a software objects or
24 a vendor of said one object, watermarking authority.
25